09/807824

PCT/JP00/05543

18.08.00

REC'D 04 SEP 2000

WIPO PCT

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　８月２０日

出願番号
Application Number: 平成１１年特許願第２３４３７１号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年　６月２９日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０４９９７７

【書類名】　特許願

【整理番号】　9900417005

【提出日】　平成11年 8月20日

【あて先】　特許庁長官　殿

【国際特許分類】　G11B　7/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　浅野　智之

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　大澤　義知

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100067736

【弁理士】

【氏名又は名称】　小池　晃

【選任した代理人】

【識別番号】　100086335

【弁理士】

【氏名又は名称】　田村　榮一

【選任した代理人】

【識別番号】　100096677

【弁理士】

【氏名又は名称】　伊賀　誠司

【手数料の表示】

【予納台帳番号】　019530

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報記録／再生システム、情報記録／再生装置、情報記録／再生方法及び情報記録媒体

【特許請求の範囲】

【請求項１】　セキュリティモジュールを有する情報記録媒体と、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体に記録、あるいは、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体から再生する情報記録／再生装置とを備え、

情報記録時、又は情報再生時に上記情報記録／再生装置とセキュリティモジュールとが公開鍵暗号技術を用いた相互認証プロトコルを実行することを特徴とする情報記録／再生システム。

【請求項２】　上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報（ID）がリボケーションリストに掲載されていないことを確認することを特徴とする請求項１記載の情報記録／再生システム。

【請求項３】　上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリストのバージョンナンバーを教え合い、新しいリボケーションリストを持つものがそれを他方に送り、古いリボケーションリストを持つものは送られた新しいリボケーションリストを用いて自分のリボケーションリストを置き換えることを特徴とする請求項１記載の情報記録／再生システム。

【請求項４】　データの記録時又は再生時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化する暗号鍵を一方が暗号化して他方に送ることを特徴とする請求項１記載の情報記録／再生システム。

【請求項５】　データの記録時又は再生時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを一方が暗号化して他方に送ることを特徴とする請求項１記

載の情報記録／再生システム。

【請求項６】　データを格納する情報記録媒体への書き込み、読み出しのアクセスは、上記セキュリティモジュールを介して行われることを特徴とする請求項１記載の情報記録／再生システム。

【請求項７】　データの記録時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いて上記情報記録／再生装置がデータを暗号化してセキュリティモジュールに送り、上記セキュリティモジュールは、共有された鍵を用いてこれを復号して平文データを得た後に、暗号鍵を用いてデータを暗号化して情報記録媒体に格納することを特徴とする請求項６記載の情報記録／再生システム。

【請求項８】　データの再生時に、上記セキュリティモジュールが暗号化されて情報記録媒体に格納されているデータを読み出し、暗号鍵を用いてこれを復号して平文データを得た後、上記情報記録／再生装置とセキュリティモジュールが鍵共有プロトコルを実行した結果共有された鍵を用いてデータを上記セキュリティモジュールが暗号化して情報記録／再生装置に送ることを特徴とする請求項６記載の情報記録／再生システム。

【請求項９】　データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた相互認証プロトコルを実行するセキュリティモジュールを有することを特徴とする情報記録媒体。

【請求項１０】　上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、情報記録／再生装置の識別情報（ID）がリボケーションリストに掲載されていないことを確認することを特徴とする請求項９記載の情報記録媒体。

【請求項１１】　上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリストのバージョンナンバーを情報記録／再生装置に送り、これと上記情報記録／再生装置が送ったリボケーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはリボケーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリストを現在自分が持っているものと置き換える処

理を行うことを特徴とする請求項９記載の情報記録媒体。

【請求項１２】　上記セキュリティモジュールが管理する暗号鍵を用いて暗号化されたデータを格納することを特徴とする請求項９記載の情報記録媒体。

【請求項１３】　上記セキュリティモジュールは、データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、データを暗号化する暗号鍵を情報記録／再生装置に送信あるいは情報記録／再生装置から受信することを特徴とする請求項９記載の情報記録媒体。

【請求項１４】　データの書き込み及び読み出しの処理が上記セキュリティモジュールを介して行われることを特徴とする請求項９記載の情報記録媒体。

~~【請求項１５】　上記セキュリティモジュールは、データの記録時に、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて受信したデータを復号し、さらに別の鍵を用いてデータを暗号化することを特徴とする請求項１４記載の情報記録媒体。~~

【請求項１６】　データの再生時に、記録媒体からデータを読み出して暗号鍵１を用いて復号した後、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、共有した鍵を用いてデータを暗号化して情報記録／再生装置に送信することを特徴とする請求項１４記載の情報記録媒体。

【請求項１７】　データの記録時及び再生時に、情報記録媒体のセキュリティモジュールとの間で公開鍵暗号を用いた相互認証プロトコルを実行する制御手段を備えることを特徴とする情報記録／再生装置。

【請求項１８】　上記制御手段は、上記相互認証プロトコルを実行するときに、上記セキュリティモジュールの識別情報（ID）がリボケーションリストに掲載されていないことを確認することを特徴とする請求項１７記載の情報記録／再生装置。

【請求項１９】　上記制御手段は、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリストのバージョンナンバーをセキュリティモジュールに送り、これと上記セキュリティモジュールが送ったリボケーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはリボ

ケーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項１７記載の情報記録／再生装置。

【請求項２０】　上記制御手段は、データの記録時及び再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、データを暗号化する暗号鍵を上記セキュリティモジュールに送信あるいは上記セキュリティモジュールから受信することを特徴とする請求項１７記載の情報記録／再生装置。

【請求項２１】　上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータを暗号化して情報記録媒体に格納することを特徴とする請求項１７記載の情報記録／再生装置。

【請求項２２】　上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータを暗号化して上記セキュリティモジュールに送信することを特徴とする請求項１７記載の情報記録／再生装置。

【請求項２３】　上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータの暗号化に用いる暗号鍵を暗号化して上記セキュリティモジュールに送信し、又は共有した鍵を用いて暗号化された暗号鍵を上記セキュリティモジュールから受信し、上記暗号鍵を用いてデータを暗号化して上記セキュリティモジュールに送信することを特徴とする請求項１７記載の情報記録／再生装置。

【請求項２４】　上記制御手段は、データの再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、上記セキュリティモジュールから送られたデータを復号することを特徴とする請求項１７記載の情報記録／再生装置。

【請求項２５】　上記制御手段は、データの再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有し

た鍵を用いて、データの暗号化に用いる暗号鍵を暗号化してセキュリティモジュールに送信し、又は共有した鍵を用いて暗号化された暗号鍵を上記セキュリティモジュールから受信し、上記暗号鍵を用いて上記セキュリティモジュールから送られたデータを復号することを特徴とする請求項１７記載の情報記録／再生装置。

【請求項２６】　情報記録／再生装置により情報記録媒体にデータを記録、あるいは情報記録媒体からデータを再生する情報記録／再生方法において、

情報記録媒体が有するセキュリティモジュールと情報記録／再生装置が公開鍵暗号を用いた相互認証プロトコルを実行するステップを有することを特徴とする情報記録／再生方法。

【請求項２７】　上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報（ID）がリボケーションリストに掲載されていないことを確認するステップを有することを特徴とする請求項２６記載の情報記録／再生方法。

【請求項２８】　上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリストのバージョンナンバーを教えるステップと、新しいリボケーションリストを持つものがそれを他方に送るステップと、古いリボケーションリストを持つものは送られた新しいリボケーションリストを用いて自分のリボケーションリストを置き換えるステップを有することを特徴とする請求項２６記載の情報記録／再生方法。

【請求項２９】　データの記録時又は再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを実行するステップと、共有された鍵を用いてデータを暗号化する暗号鍵を一方が暗号化して他方に送るステップを有することを特徴とする請求項２６記載の情報記録／再生方法。

【請求項３０】　データの記録時又は再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを行うステップと、共有された鍵を用いてデータを一方が暗号化して他方に送るステップを有することを特徴とする請求項２６記載の情報記録／再生方法。

【請求項３１】　データの記録時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを実行するステップと、共有された鍵を用いてデータを情報記録／再生装置が暗号化して他方に送るステップと、セキュリティモジュールが受信したデータを共有された鍵を用いて復号するステップと、セキュリティモジュールが上記復号したデータを鍵を用いて暗号化するステップと、セキュリティモジュールが上記暗号化したデータを情報記録媒体に格納するステップを有することを特徴とする請求項２６記載の情報記録／再生方法。

【請求項３２】　データの再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを行つて鍵を共有するステップと

セキュリティモジュールが情報記録媒体からデータを読み出して鍵を用いて復号するステップと、セキュリティモジュールが上記復号後のデータを共有した鍵を用いて暗号化するステップと、セキュリティモジュールが上記暗号化後のデータを情報記録／再生装置に送信するステップとを有することを特徴とする請求項２６記載の情報記録／再生方法。

【請求項３３】　外部装置とインタフェースをとるためのインタフェース機能と、乱数を生成するための乱数生成機能と、情報を保存するための記憶機能と、公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行う演算機能を有するセキュリティモジュールを備えることを特徴とする情報記録媒体。

【請求項３４】　上記セキュリティモジュールは、データを記録するための記録領域にアクセスするためのインタフェース機能を備えることを特徴とする請求項３３記載の情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、安全にデータを授受することを可能にした情報記録／再生システム、情報記録装置及び情報再生装置等に関する。

【０００２】

【従来の技術】

近年、情報をデジタル的に記録する記録装置及び記録媒体が普及しつつある。これらの記録装置及び記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録装置及び記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

【０００３】

このような著作権保護のためのシステムとして、例えば、ミニディスク（MD）（商標）システムにおいては、ＳＣＭＳ(Serial Copy Management System) と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、copy free、copy once allowed、又はcopy prohibited のうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、ＳＣＭＳを検出し、これが、copy prohibited であれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。

【０００４】

このようにして、ミニディスクシステムにおいては、ＳＣＭＳを用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

【０００５】

また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk (DVD)（商標）システムにおける、コンテンツスクランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録装置だけが暗号鍵を与えられ、これにより暗号化されたデータを復号し、意味のあるデータを得ることができ

るようになされている。そして、記録装置は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、ＤＶＤシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【０００６】

【発明が解決しようとする課題】

上記のミニディスクシステムが採用している方式では、ＳＣＭＳがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録するなどの動作規定に従わない記録装置が、不正に製造されてしまう。

【０００７】

また、上記のＤＶＤシステムが採用している方式は、ＲＯＭメディアに対しては有効であるが、ユーザがデータを記録可能なＲＡＭメディアにおいては有効ではない。ＲＡＭメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録装置で動作するディスクを新たに作ることができるからである。

【０００８】

そこで、本件出願人が先に出願した特願平１０－２５３１０号の特許出願においては、個々の記録媒体を識別するための情報（以下、媒体識別情報とよぶ）を記録媒体に持たせ、この情報はライセンスを受けた装置しかアクセスできないようにしている。すなわち、記録媒体上のデータは媒体識別情報と、ライセンスを受けることによって得られる秘密に基づく鍵によって暗号化し、ライセンスを受けていない装置はデータを読み出しても意味のないものとしている。さらに装置にライセンスを与える際にはその動作を規定し、不正コピーを行わないようにする。ライセンスを得ていない装置は媒体識別情報にアクセスできず、また媒体識別情報は個々の媒体ごとに個別の値になっているため、ライセンスを受けていない装置がアクセス可能なすべての情報を新たな媒体にコピーしたとしても、そのようにして作られた媒体は、ライセンスを受けていない装置でもライセンスを受けた装置でも正しく情報が読み出せないようにしている。

【０００９】

しかしながら、ある記録装置によって情報が記録された記録媒体が、他の装置で再生可能であることを保証するために、記録媒体上のデータを暗号化する暗号鍵は、システム全体で共通の秘密（マスターキー）に基づいて生成されるようになっている。これはすなわち、一つの装置が攻撃されてマスターキーが露呈してしまうと、そのシステムの任意の装置によって記録されたすべてのデータの暗号が解かれ、システム全体が壊滅する恐れがあることを意味している。

【００１０】

そこで、本発明の目的は、暗号鍵を安全に保管することができるようにした情報記録／再生システム、情報記録／再生装置、情報記録／再生方法及び情報記録媒体を提供することにある。

【００１１】

また、本発明の他の目的は、不正な機器にデータを漏らすことのないようにした情報記録／再生システム、情報記録／再生装置、情報記録／再生方法及び情報記録媒体を提供することにある。

【００１２】

また、本発明の他の目的は、正当な機器だが攻撃されてその機器の秘密が露呈してしまった機器にデータを与えることも防ぐことができるようにした情報記録／再生システム、情報記録／再生装置、情報記録／再生方法及び情報記録媒体を提供することにある。

【００１３】

さらに、本発明の他の目的は、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができるようにした情報記録／再生システム、情報記録／再生装置、情報記録／再生方法及び情報記録媒体を提供することにある。

【００１４】

【課題を解決するための手段】

本発明では、情報記録媒体にセキュリティモジュールを持たせる。情報記録媒体上に記録されるデータは、個々のデータごとに異なる暗号鍵で暗号化され、暗

号鍵はセキュリティモジュールが安全に保管する。また、セキュリティモジュールは記録／再生装置と公開鍵暗号技術を用いた相互記証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにする。さらに、信頼できるセンタが発行するリボケーションリストを活用することにより、正当な装置だが攻撃されてその装置の秘密が露呈してしまった装置にデータを与えることも防ぐことができるようにする。

【００１５】

すなわち、本発明に係る情報記録／再生システムは、セキュリティモジュールを有する情報記録媒体と、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体に記録、あるいは、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体から再生する情報記録／再生装置とを備え、情報記録時、又は情報再生時に上記情報記録／再生装置とセキュリティモジュールとが公開鍵暗号技術を用いた相互認証プロトコルを実行することを特徴とする。

【００１６】

また、本発明に係る情報記録媒体は、データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた相互認証プロトコルを実行するセキュリティモジュールを有することを特徴とする。

【００１７】

また、本発明に係る情報記録／再生装置は、データの記録時及び再生時に、情報記録媒体のセキュリティモジュールとの間で公開鍵暗号を用いた相互認証プロトコルを実行する制御手段を備えることを特徴とする。

【００１８】

また、本発明は、情報記録／再生装置により情報記録媒体にデータを記録、あるいは情報記録媒体からデータを再生する情報記録／再生方法において、情報記録媒体が有するセキュリティモジュールと情報記録／再生装置が公開鍵暗号を用いた相互認証プロトコルを実行するステップを有することを特徴とする。

【００１９】

さらに、本発明に係る情報記録媒体は、外部装置とインタフェースをとるためのインタフェース機能と、乱数を生成するための乱数生成機能と、情報を保存するための記憶機能と、公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行う演算機能を有するセキュリティモジュールを備えることを特徴とする。

【００２０】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

【００２１】

図１は、本発明を適用した光ディスク情報記録媒体１０の構成例を示している。

【００２２】

この光ディスク情報記録媒体１０は、カートリッジ１１内に、データを記録する光ディスク１２と、セキュリティモジュール１３を備えている。図２は、上記セキュリティモジュール１３の構成例を示している。

【００２３】

セキュリティモジュール１３は、図２に示すように、モジュール外の装置とデータの授受をするための接触式あるいは非接触式のインタフェース部３１、演算を行うための演算部３２、疑似乱数を発生させる乱数発生部３３、不揮発性メモリ３４と、それらを制御するための制御部３５を備えている。

【００２４】

図３は、本発明を適用した光ディスク記録／再生装置１００の構成例を示している。

【００２５】

この光ディスク記録／再生装置１００は、上記光ディスク情報記録媒体１０を介してデータの記録／再生を行うもので、カートリッジ１１内の光ディスク１２を回転させるスピンドルモータ１０１、光学ヘッド１０２、サーボ回路１０３、記録／再生回路１０４、これらを制御する制御部１０５、この制御部１０５に接続された入力部１０６、乱数発生部１０７やインタフェース部１０８などを備え

ている。

【００２６】

スピンドルモータ１０１は、サーボ回路１０３によって制御され、光ディスク１２を回転させる。光学ヘッド１０２は、レーザビームを光ディスク１２に照射することで、データの記録／再生を行う。サーボ回路１０３は、スピンドルモータ１０１を駆動することにより、光ディスク１２を所定の速度で（例えば線速度一定で）回転させる。また、サーボ回路１０３は、光学ヘッド１０２のトラッキング及びフォーカシングの他、スレッドサーボを制御する。

【００２７】

そして、記録／再生回路１０４は、制御部１０５により動作モードが切り換えられる暗号化部１０４Ａと復号部１０４Ｂを有する。暗号化部１０４Ａは、記録モード時に、外部から記録信号の供給を受け取ると、これを暗号化し、光学ヘッド１０２に供給して、光ディスク１２に記録させる。復号部１０４Ｂは、再生モード時に、光学ヘッド１０２により光ディスク１２から再生されたデータを復号し、外部に再生信号として出力する。

【００２８】

また、入力部１０６は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。制御部１０５は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。乱数発生部１０７は、制御部１０５の制御により、所定の乱数を発生する。インタフェース１０８部は、接触式あるいは非接触式であり、情報記録媒体１０のセキュリティモジュール１３とデータの授受を行う。

【００２９】

さらに、この光ディスク記録／再生装置１００は、演算部１０９と不揮発性メモリ１１０を備えている。

【００３０】

光ディスク情報記録媒体１０のセキュリティモジュール１３と光ディスク記録／再生装置１００は、１台ごとに個別の識別コード(ＩＤ)と、ＩＤに対応する公開鍵暗号系の秘密鍵と公開鍵、さらに、公開鍵証明書を信頼できるセンタ(Trust

ed Center: TC)から与えられており、それぞれの不揮発性メモリ３４，１１０にこれらを格納しておく。特に、秘密鍵は外部に漏れないように安全に格納する。

【００３１】

ここで、公開鍵証明書は、ＩＤと公開鍵を含む情報にＴＣがデジタル署名を施したデータである。

【００３２】

また、デジタル署名技術は、あるデータを生成したのがあるユーザであることを証明できる技術であり、例えばＩＥＥＥ　Ｐ１３６３　で使用されているElliptic Curve Digital Signature Algorithm (EC-DSA) 方式などがよく知られている。

【００３３】

この実施の形態では、公開鍵証明書に含まれるTCのデジタル署名を検証するために、システム全体で共通であるTCの公開鍵を光ディスク情報記録媒体１０と光ディスク記録／再生装置１００の不揮発性メモリ３４，１１０に格納する。

【００３４】

上記光ディスク情報記録媒体１０のセキュリティモジュール１３と光ディスク記録／再生装置１００は、その不揮発メモリ３４，１１０に、図４に示すリボケーションリストを格納する領域を有する。

【００３５】

リボケーションリストは、単調増加であるそのバージョンナンバーと、秘密鍵が露呈した光ディスク情報記録媒体あるいは光ディスク記録／再生装置のIDにTCがデジタル署名を施したものである。

【００３６】

光ディスク情報記録媒体１０のセキュリティモジュール１３の不揮発メモリ３４の容量が小さく、リボケーションリストを格納できない場合には、不揮発メモリ３４ではなく、光ディスク１２部分にリボケーションリストを格納してもよい。

【００３７】

光ディスク記録／再生装置１００は、それが工場から出荷される際に、最新版

のリボケーションリストを与えられ不揮発性メモリ１１０に格納することが望ましい。

【００３８】

次に、図５を用いて、光ディスク記録／再生装置１００が光ディスク情報記録媒体１０にデータを記録する手順を説明する。

【００３９】

光ディスク記録／再生装置１００と光ディスク情報記録媒体１０のセキュリティモジュール１３は、それぞれ、ＴＣから与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書と、リボケーションリストを持っている。

【００４０】

まず、光ディスク記録／再生装置１００が光ディスク情報記録媒体１０のセキュリティモジュール１３に対し、これからデータの記録を行うことを示す記録コマンドと、１回１回の記録を識別するために個別に割り当てるRecording-IDを送る（手順Ｒ１）。

【００４１】

上記記録コマンドをトリガーとして、光ディスク記録／再生装置１００が光ディスク情報記録媒体１０のセキュリティモジュール１３は、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する（手順Ｒ２）。

【００４２】

公開鍵暗号技術を用いた相互認証プロトコルは、相手の装置が正しい（ＴＣから承認を得た）公開鍵と秘密鍵のペアを持っていることをお互いに確認するプロトコルであり、例えばＩＥＥＥ　Ｐ１３６３で規格化作業中のElliptic Curve Digital Signature Algorithm (EC-DSA) を用いることによって構成することができる。

【００４３】

上記公開鍵暗号技術を用いた相互認証プロトコルにおいては、双方の装置が、乱数発生機能を用いて乱数を発生させること、不揮発性メモリに格納されている自己の秘密鍵及び公開鍵証明書を読み出すこと、公開鍵暗号技術に基づく演算を演算機能で行うこと、が必要となる。

【００４４】

なお、公開鍵暗号技術を用いた相互認証プロトコルに対し、共通鍵暗号技術を用いた相互認証プロトコルも広く知られているが、これはその名の通り、プロトコルを行う２者が共通の鍵を持っていることを前提とするプロトコルである。共通鍵暗号技術を用いた相互認証プロトコルを採用しようとした場合、記録鍵体と記録／再生装置のインターオペラビリティを確保する必要があるため、システム全体で共通の鍵をすべてのセキュリティモジュール１３と光ディスク記録／再生装置１００が持つ必要がある。この場合、ひとつのセキュリティモジュールあるいは光ディスク記録／再生装置が攻撃を受けて鍵が露呈してしまうと、その影響がシステム全体に広まってしまうという問題がある。

【００４５】

これに対し、公開鍵暗号技術を用いた相互認証プロトコルにおいては、各装置及び各セキュリティモジュールが持つ鍵は個別であり、しかも後述のリボケーションリストを使用できるため、ひとつの装置の鍵が露呈したとしても、その装置だけをシステムから排除することができるので、影響が小さく押さえられるという利点がある。

【００４６】

公開鍵暗号技術を用いた鍵共有プロトコルは、２者間で安全に秘密情報を共有するためのプロトコルであり、やはりＩＥＥＥ　Ｐ１３６３で規格化作業中のElliptic Curve　Diffie Hellman　(EC-DH) を用いることによって構成することができる。

【００４７】

公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実際に用いている例としては、ＩＥＥＥ　１３９４パス上のコンテンツプロテクション方式のひとつである、ソニー、松下、日立、東芝、インテルの５社によって開発された、Digital Transmission Content Protection 規格（この規格そのものはライセンスを受けないと見ることができないが、その概要を記したWhite Paper を、ライセンス組織であるDigital Transmission Licensing Administrator (DTLA) のウエブページであるhttp://www。dtcp. comから誰でも取得することが可能である）のF

ull Authentication and Key Exchange プロトコルを挙げることができる。このプロトコルは、おおまかには、下記のステップＳ１～Ｓ４で構成される。

【００４８】

（Ｓ１）　乱数発生器を用いて乱数を発生させ、不揮発性メモリから読み出した自分の公開鍵証明書とともに他方に送る。

（Ｓ２）　相手の公開鍵証明書の正当性を公開鍵暗号技術に基づく演算を行って確かめる。

（Ｓ３）　鍵共有のための、公開鍵暗号技術に基づく演算（第１段階）を行い、公開鍵暗号技術に基づく演算を行って作成した自分のデジタル署名文とともに相手に送る。

（Ｓ４）　相手から送られたＳ３．のデータについて、公開鍵暗号技術に基づく演算を行って相手のデジタル署名の検証を行い、鍵共有のための、公開鍵暗号技術に基づく演算（第２段階）を行って共有鍵の値を計算する。

【００４９】

本方式においては、相互認証を行う際に、相手の装置が正しい秘密鍵、公開鍵ペアを持っていることのみならず、自分が持つリボケーションリスト（ブラックリスト）に相手の装置のIDがあげられていないことを確認する。これにより、出荷時には正当に鍵を持っていたが、それが例えばリバースエンジニアリングなどの攻撃を受け、鍵が露呈してしまった装置のＩＤがリボケーションリストに載せられているので、データを渡してはいけない装置にはデータを渡さずにすむようになる。

【００５０】

さらに、自分が持っているリボケーションリストのバージョンナンバーを交換する。

【００５１】

もし何れかの装置が他方のリボケーションリストより新しいリボケーションリストを持っていた場合、その装置は自分のリボケーションリストを他方に送る。古いリボケーションリストを持っている装置は新しいものを持っている装置からリボケーションリストを送ってもらい、その正当性を検証した後で自分が持つリ

ボケーションリストを送られた新しいものに更新する。

【００５２】

なお、このリボケーションリストの送付は、後述のデータの記録と順序が前後してもかまわない。

【００５３】

さて、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルの結果、光ディスク記録／再生装置１００とセキュリティモジュール１３は、安全にある値を共有する。

【００５４】

この共有される値をSession key（Kse）と呼ぶことにする。

【００５５】

次に、データを暗号化する暗号鍵（Content key, Kc）を決定するが、この方法には、例えば、次の方法（１）～（４）のうちのひとつを用いればよい。

【００５６】

（１）　Ｋｓｅ＝Ｋｃとする。セキュリティモジュール１３はＫｃを安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３があらかじめ格納している鍵（Storage key, Kst）を用いてＫｃを暗号化した値Ｅｎｃ（Kst, Kc）を光ディスク記録／再生装置１００に送り、光ディスク１２に記録させる。

（２）　セキュリティモジュール１３があらかじめ格納している鍵（Storage key, Kst）をＫｃとする。この場合、セキュリティモジュール１３がＫｓｔをＫｓｅで暗号化して光ディスク記録／再生装置１００に送る。

（３）　セキュリティモジュール１３がそのデータ用のＫｃを乱数発生器などを用いて新たに発生させる。この場合、セキュリティモジュール１３がＫｃをＫｓｅで暗号化して光ディスク記録／再生装置１００に送る。セキュリティモジュール１３はＫｃを安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３があらかじめ格納している鍵（Storage key, Kst）を用いてＫｃを暗号化した値Ｅｎｃ（Ｋｓｔ，Ｋｃ）を光ディスク記録／再生装置１００に送り、光ディスク１２に記録させる。

（４）　光ディスク記録／再生装置１００がそのデータ用のＫｃを乱数発生器などを用いて新たに発生させる。この場合、光ディスク記録／再生装置１００がＫｃをＫｓｅで暗号化してセキュリティモジュール１３に送る。セキュリティモジュール１３はＫｃを安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３があらかじめ格納している鍵（Storage key, Kst）を用いてKcを暗号化した値Enc（Kst, Kc）を光ディスク記録／再生装置１００に送り、光ディスク１３に記録させる。

【００５７】

上記方法（１）～（４）のいずれかを用いてＫｃを決定したら、光ディスク記録／再生装置１００は記録媒体に記録するデータをＫｃで暗号化し、暗号化されたデータＥｎｃ（Kc, data）を光ディスク１２に記録する（手順Ｒ３）。

【００５８】

また、上記Ｋｃ又は暗号化したＫｃをセキュリティモジュール１３の不揮発性メモリ３４又は光ディスク１２に記録する際には、Recording - ID を検索用のキーとするために一緒に記録したり、データが記録される光ディスク１２のセクタと同一のセクタに暗号化したＫｃを記録するなどして、データとＫｃの対応がとれるようにしておく。なお、このＫｃの管理、伝送とデータの暗号化には、その処理速度の観点から共通鍵暗号アルゴリズムを使用することが考えられる。

【００５９】

共通鍵暗号アルゴリズムは、暗号化と復号の処理に同一の暗号鍵を用いる暗号アルゴリズムであり、ＦＩＰＳ４６－２で米国の標準に指定されているData Encryption Standard (DES) をその例として挙げることできる。

【００６０】

また、上記方法（４）の場合には、光ディスク記録／再生装置１００がＫｃを決められるため、光ディスク記録／再生装置１００はあらかじめデータを暗号化しておくことが可能になる。

【００６１】

以上の手順を用いて、データを光ディスク１２に記録する。

【００６２】

次に、図６を用いて、光ディスク記録／再生装置１００が光ディスク１２からデータを再生する手順を説明する。

【００６３】

光ディスク記録／再生装置１００と光ディスク記録媒体１０のセキュリティモジュール１３は、それぞれTCから与えられたID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書と、リボケーションリストを持っている。

【００６４】

また、光ディスク記録／再生装置１００は、再生すべきデータに付与されたRecording-IDを知っているものとする。

【００６５】

まず、光ディスク記録／再生装置１００がセキュリティモジュール１３に対し、これからデータの再生を行うことを示す再生コマンドとRecording-IDを送る（手順Ｐ１）。

【００６６】

上記再生コマンドをトリガーとして、光ディスク記録／再生装置１００とセキュリティモジュール１３は公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを行う（手順Ｐ２）。

【００６７】

このプロトコルの内容は、データの記録時に行うものと同様であり、他方の装置が持つ公開鍵、秘密鍵が正しいことの検証、リボケーションリストにIDが載せられていないことの確認をお互いに行い、Session key (Kse) を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。どちらかの装置が相対的に新しいリボケーションリストを持っていた場合には、それを他方の装置に送り、送られた装置はそれを用いて自分のリボケーションリストを更新することも同様である。また、リボケーションリストを送る処理が下記のデータの読み出しと前後してよいことも同様である。

【００６８】

次に、データを光ディスク１２から読み出す前に、このデータを暗号化してい

る暗号鍵Ｋｃを光ディスク記録／再生装置１００が知ることが必要になる。

【００６９】

Ｋｃは、セキュリティモジュール１３が安全にその内部の不揮発性メモリ３４に格納しているか、セキュリティモジュール１３があらかじめ格納している鍵（Storage key、Kst）を用いてＫｃを暗号化した値Ｅｎｃ（Kst，Kc）が光ディスク１２に記録されている。

【００７０】

前者の場合であれば、セキュリティモジュール１３は不揮発性メモリ３４に格納されているＫｃをＫｓｅで暗号化して光ディスク記録／再生装置１００に送り、光ディスク記録／再生装置１００がＫｓｅでこれを復号してＫｃを得る。

【００７１】

後者の場合であれば、光ディスク記録／再生装置１００は、光ディスク１２からＥｎｃ（Kst，Kc）を読み出し、これをセキュリティモジュール１３に送る。セキュリティモジュール１３はＫｓｔを用いてこれを復号してＫｃを得、これをＫｓｅで暗号化したＥｎｃ（Kse，Kc）を光ディスク記録／再生装置１００に送る。光ディスク記録／再生装置１００はこれをＫｓｅで復号してＫｃを得る。

【００７２】

このようにして、光ディスク記録／再生装置１００は、データを暗号化している暗号鍵Ｋｃを得ることができる。

【００７３】

次に、光ディスク記録／再生装置１００は光ディスク１２からＫｃを用いて暗号化されているデータＥｎｃ（Kc，data）を読み出し、Kcを用いてこれを復号し使用する（手順Ｐ３）。

【００７４】

以上が、光ディスク１２からデータを読み出す処理である。

【００７５】

次に、本発明の別の実施の形態を説明する。

【００７６】

図７は、本発明を適用した不揮発性メモリ情報記録媒体２０の構成例を示して

いる。

【００７７】

この不揮発性メモリ情報記録媒体２０は、カートリッジ２１内に、データを記録する電気的に消去可能な不揮発性メモリ（具体的には例えば、Flash ROM やEEPROMなど）２２と、セキュリティモジュール２３を備えている。

【００７８】

上記セキュリティモジュール２３は、その構成例を図８に示すように、外部インタフェース部４１、演算部４２、乱数発生部４３、不揮発性メモリ４４、制御部４５、記録媒体インタフェース部４６からなる。

【００７９】

すなわち、このセキュリティモジュール２３は、図２に示したセキュリティモジュール１３とほぼ同じ構成であるが、図２のインタフェース部３１はこのセキュリティモジュール２３では外部インタフェース部４１とし、外部装置とのインタフェースとなっている。

【００８０】

また、カートリッジ２１内の不揮発性メモリ２２とのインタフェースをとるための記録媒体インタフェース（例えば、Flash ROM インタフェース）４６を持ち、不揮発性メモリ２２への情報の記録（書き込み）、再生（読み出し）はセキュリティモジュール２３を介して行われる。

【００８１】

セキュリティモジュール２３内部の不揮発性メモリ４４は、秘密性の必要な情報や耐改ざん性が必要な情報など、重要な情報を格納するのに用いられるが、もしこのメモリ４４の容量が十分でない場合には、セキュリティモジュール２３外の、一般データを記録するための不揮発性メモリ２２にこれらの重要な情報を記録することもできる。この場合、秘密性の必要な情報については、セキュリティモジュール２３内の不揮発性メモリ４４に安全に格納してあるstorage key を鍵として暗号化するなどの方法を用いて保護し、耐改ざん性の必要な情報については、重要な情報を記録する不揮発性メモリ２２のブロックのIntegrity Check Value（ICV）を計算し、セキュリティモジュール２３内の不揮発性メモリ４４に格

納しておき、セキュリティモジュール２３外の不揮発性メモリ２２から情報を読み出す際に再びそのブロックのＩＣＶを計算して格納してある値と比較することによって情報が改ざんされていないことを確認するなどの保護をかける。

【００８２】

ＩＣＶは、あるデータのIntegrity（改ざんされていないこと）を保証するために、データと、何らかの秘密（この場合、例えばセキュリティモジュール２３のstoragekey）を入力としてあらかじめ定められたアルゴリズムによって計算される値であり、上記の秘密を知っているものしか任意のデータに対するＩＣＶを計算することが事実上できないため、データが変更された場合には読み出し時に同様の方法で計算されるＩＣＶと記録時に計算されてセキュリティモジュール２３内に格納されている値が異なるためデータが変更された事実をセキュリティモジュール２３が知ることができる。

【００８３】

ＩＣＶを計算するアルゴリズムとしては、公開鍵暗号技術を用いたデジタル署名アルゴリズムや、共通鍵暗号技術を用いたMessage Authentication Code 作成アルゴリズム、鍵つきハッシュ関数を用いるアルゴリズムなどがある。

【００８４】

ICVについては、例えば、Menezesの他、「Handbook of applied cryptography」、CRC、ISBN 0－8493-8523-7、pp. 352－368に群しい解説がある。

【００８５】

図９は、本発明を適用した不揮発メモリ記録媒体２０の記録／再生装置２００の構成例を表している。この図９に示した記録／再生装置２００は、入出力端子２０１、制御部２０５、入力部２０６、乱数発生部２０７、インタフェース部２０８、演算部２０９、不揮発性メモリ２１０などからなる。

この記録／再生装置２００は、図３に示した光ディスク記録／再生装置１００とほぼ同じであるが、スピンドルモータ１０１、光学ヘッド１０２やサーボ回路１０３など光ディスク１２用の構成要素のかわりにセキュリティモジュール２３にアクセスするためのインタフェース部２０８が、セキュリティモジュール２３を介して不揮発メモリ記録媒体２０への記録／再生のためのインタフェースも兼

用する。不揮発メモリ記録媒体２０は、入出力端子２４，２０１を介して記録／再生装置２００と電気的に接続される。

【００８６】

次に、図１０を用いて、記録／再生装置２００が不揮発メモリ記録媒体２０にデータを記録する手順を説明する。

【００８７】

図５で示した例と同様に、記録／再生装置２００と不揮発メモリ記録媒体２０のセキュリティモジュール２３は、それぞれ、ＴＣから与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書と、リボケーションリストを持っている。

【００８８】

まず、記録／再生装置２００がセキュリティモジュール２３に対し、これからデータの記録を行うことを示す記録コマンドと、１回１回の記録を識別するために個別に割り当てるRecording-IDを送る（手順Ｒ１１）。

【００８９】

上記記録コマンドをトリガーとして、記録／再生装置２００とセキュリティモジュール２３は公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する（手順Ｒ１２）。このプロトコルの内容は、上述の光ディスク記録／再生装置１００おけるデータの記録時に行うものと同様であり、他方の装置が持つ公開鍵、秘密鍵が正しいことの検証、リボケーションリストにIDが載せられていないことの確認を互いに行い、Session key (Kse) を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。どちらかの装置が相対的に新しいリボケーションリストを持っていた場合には、それを他方の装置に送り、送られた装置はそれを用いて自分のリボケーションリストを更新することも同様である。また、リボケーションリストを送る処理が下記のデータの読み出しと前後してよいことも同様である。

【００９０】

次に、データを暗号化する暗号鍵 (Content key, Kc) を決定するが、この方法には例えば、次の方法（１１）～（１４）のうちのひとつを用いればよい。

【００９１】

（１１）　Ｋｓｅ＝Ｋｃとする。セキュリティモジュール２３はＫｃを安全にその内部の不揮発性メモリ４４に格納するか、セキュリティモジュール２３があらかじめ格納している鍵（Storage key, Kst）を用いてKcを暗号化した値Ｅｎｃ（Kst, Kc）をモジュール２３外の不揮発性メモリ２２に格納する。

（１２）　セキュリティモジュール２３があらかじめ格納している鍵（Storage key, Kst）をＫｃとする。この場合、セキュリティモジュール２３がＫｓｔをＫｓｅで暗号化して記録／再生装置２００に送る。

（１３）　セキュリティモジュール２３がそのデータ用のＫｃを乱数発生器などを用いて新たに発生させる。この場合、セキュリティモジュール２３がＫｃをＫｓｅで暗号化して記録／再生装置２００に送る。セキュリティモジュール２３はＫｃを安全にその内部の不揮発性メモリ４４に格納するか、セキュリティモジュール２３があらかじめ格納している鍵（Storage key, Kst）を用いてＫｃを暗号化した値Ｅｎｃ（Kst, Kc）をモジュール２３外の不揮発性メモリ２２に格納する。

（１４）　記録／再生装置２００がそのデータ用のＫｃを乱数発生器などを用いて新たに発生させる。この場合、記録／再生装置２００がＫｃをＫｓｅで暗号化してセキュリティモジュール２３に送る。セキュリティモジュール２３はＫｃを安全にその内部の不揮発性メモリ４４に格納するか、セキュリティモジュール２３があらかじめ格納している鍵（Storage key, Kst）を用いてＫｃを暗号化した値Ｅｎｃ（Kst、Kc）をモジュール２３外の不揮発性メモリ２２に格納する。

【００９２】

上記方法（１１）～（１４）のいずれかを用いてＫｃを決定したら、記録／再生装置２００は不揮発メモリ記録媒体２０に記録するデータをＫｃで暗号化し、暗号化されたデータＥｎｃ（Kc, data）をセキュリティモジュール２３に伝送する（手順Ｒ１３）。

【００９３】

セキュリティモジュール２３は送られたＥｎｃ（Kc, data）をデータ用の不揮発性メモリ２２に格納する。

【００９４】

また上記において、Ｋｃ又は暗号化したＫｃをセキュリティモジュール２３の不揮発性メモリ４４又はデータ用の不揮発性メモリ２２に記録する際には、Recording-IDを検索用のキーとするために一緒に記録したり、データが記録される不揮発性メモリのセクタと同一のセクタに暗号化したＫｃを記録するなどして、データとＫｃの対応がとれるようにしておく。

【００９５】

また、上記方法（１４）の場合には、記録／再生装置２００がKcを決められるため、記録／再生装置２００はあらかじめデータを暗号化しておくことが可能になる。

【００９６】

以上の手順を用いて、データを不揮発メモリ記録媒体２０に記録する。

【００９７】

ところで、データの記録処理を図１１のようにすることもできる。

【００９８】

すなわち、記録／再生装置２００は認証と鍵共有プロトコルでセキュリティモジュール２３と共有したSession key（Kse）を用いてデータを暗号化してセキュリティモジュール２３に送る（手順Ｒ２３）。

【００９９】

セキュリティモジュール２３は同じくＫｓｅを用いてこれを復号し平文のデータを得、次に新たに発生させたＫｃで暗号化してＥｎｃ（Kc, data）をデータ用の不揮発性メモリに記録する（手順Ｒ２４）。

【０１００】

セキュリティモジュール２３はＫｃを安全にその内部の不揮発性メモリ４４に格納するか、セキュリティモジュール２３があらかじめ格納している鍵（Storage key, Kst）を用いてＫｃを暗号化した値Ｅｎｃ（Kst, Kc）をモジュール２３外の不揮発性メモリ２２に格納する。このようにすると、セキュリティモジュール２３はデータの暗号鍵Ｋｃを記録／再生装置２００にも教えないですむようになる。

【０１０１】

以上のようにして、データを記録媒体に記録することができる。

【０１０２】

次に、図１２を用いて、記録／再生装置２００が不揮発メモリ記録媒体２０からデータを再生する手順を説明する。

【０１０３】

記録／再生装置２００と不揮発メモリ記録媒体２０のセキュリティモジュール２３は、それぞれ、ＴＣから与えられたＩＤ、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書と、リボケーションリストを持っている。また、記録／再生装置２００は、再生すべきデータに付与されたRecording-IDを知っているものとする。

【０１０４】

まず、記録／再生装置２００がセキュリティモジュール２３に対し、これからデータの再生を行うことを示す再生コマンドと、Recording-IDを送る（手順Ｐ１１）。

【０１０５】

上記再生コマンドをトリガーとして、記録／再生装置２００とセキュリティモジュール２３は公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する（手順Ｐ１２）。

【０１０６】

このプロトコルの内容は、データの記録時に行うものと同様であり、他方の装置が持つ公開鍵、秘密鍵が正しいことの検証、リボケーションリストにIDが載せられていないことの確認をお互いに行い、Session key（Kse）を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。どちらかの装置が相対的に新しいリボケーションリストを持っていた場合には、それを他方の装置に送り、送られた装置はそれを用いて自分のリボケーションリストを更新することも同様である。また、リボケーションリストを送る処理が下記のデータの読み出しと前後してよいことも同様である。

【０１０７】

次に、データを不揮発性メモリ２２から読み出す前に、このデータを暗号化し

ている暗号鍵Kcを記録／再生装置に知らせる。

【０１０８】

Ｋｃは、セキュリティモジュール２３が安全にその内部の不揮発性メモリ４４に格納しているかセキュリティモジュール２３があらかじめ格納している鍵（Storage key, Kst）を用いてKcを暗号化した値Ｅｎｃ（Kst, Kc）がデータ用の不揮発性メモリ２２に記録されている。

【０１０９】

前者の場合であれば、セキュリティモジュール２３は不揮発性メモリ４４に格納されているＫｃを Ｋｓｅで暗号化して記録／再生装置２００に送り、記録／再生装置２００がＫｓｅでこれを復号してＫｃを得る。

【０１１０】

後者の場合であれば、セキュリティモジュール２３はデータ用の不揮発性メモリ２２からＥｎｃ（Kst, Kc）を読み出し、Ｋｓｔを用いてこれを復号してＫｃを得、これをＫｓｅで暗号化したＥｎｃ（Kse, Kc）を記録／再生装置２００に送る。記録／再生装置２００はこれをKseで復号してKcを得る。

【０１１１】

このようにして、記録／再生装置２００はデータを暗号化している暗号鍵Kcを得ることができる。

【０１１２】

次に、記録／再生装置２００はデータ用の不揮発性メモリ２２からKcを用いて暗号化されているデータＥｎｃ（Kc, data）をセキュリティモジュール２３を介して読み出し（手順Ｐ１３）、Ｋｃを用いてこれを復号し使用する（手順Ｐ１４）。

【０１１３】

以上が、記録媒体からデータを読み出す処理である。

【０１１４】

ところで、データの再生処理を図１３のようにすることもできる。

【０１１５】

すなわち、セキュリティモジュール２３が記録／再生装置２００にKcを渡すこ

とはせず、セキュリティモジュール２３がデータ用の不揮発性メモリ２２から暗号化されたデータＥｎｃ（Kc, data）を読み出した後（手順２３）、Ｋｃを用いて復号して平文のデータを得、次に認証と鍵共有プロトコルで共有したSession key（Kse）でデータを暗号化してＥｎｃ（Kse, data）を記録／再生装置２００に送る（手順Ｐ２４）。

【０１１６】

記録／再生装置２００はこれをKseを用いて復号して平文データを得、使用する（手順Ｐ２５）。

【０１１７】

このようにすることにより、セキュリティモジュール２３はデータを暗号化している暗号鍵Kcを記録／再生装置２００に教える必要がなくなる。

【０１１８】

以上のようにして、記録媒体からのデータの読み出しが行える。

【０１１９】

なお、本発明を適用した情報記録媒体としては、光ディスク記録媒体１０と不揮発性メモリ記録媒体２００の例を提示したが、記録媒体はこれに限るものではなく、磁気ディスクや磁気テープ、光磁気ディスク、バッテリーバックアップされた揮発性メモリなどでもよい。

【０１２０】

【発明の効果】

以上に説明したように、本発明によれば、記録媒体にセキュリティモジュールを持たせ記録媒体上に記録されるデータは個々のデータごとに異なる暗号鍵で暗号化され、暗号鍵はセキュリティモジュールが安全に保管することができる。

【０１２１】

また、セキュリティモジュールは、データの記録時及び再生時に、記録／再生装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにすることができる。

【０１２２】

さらに、信頼できるセンタが発行するリボケーションリストを活用することにより、正当な装置だが攻撃されてその装置の秘密が露呈してしまった装置にデータを与えることも防ぐことが可能となる。

【０１２３】

このため、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことが可能である。

【図面の簡単な説明】

【図１】

本発明を適用した光ディスク情報記録媒体の構成を示す図である。

【図２】

上記光ディスク情報記録媒体に備えられるセキュリティモジュールの一例を示すブロック図である。

【図３】

本発明を適用した光ディスク情報記録／再生装置の構成を示すブロック図である。

【図４】

リボケーションリストを説明するための図である。

【図５】

上記光ディスク情報記録媒体にデータを記録する際の具体的な処理内容を示す図である。

【図６】

上記光ディスク情報記録媒体からデータを再生する際の具体的な処理内容を示す図である。

【図７】

本発明を適用した不揮発性メモリ情報記録媒体の構成を示す図である。

【図８】

上記不揮発性メモリ情報記録媒体に備えられるセキュリティモジュールの一例を示すブロック図である。

【図９】

本発明を適用した不揮発性メモリ情報記録／再生装置の構成を示すブロック図である。

【図１０】

上記不揮発性メモリ情報記録媒体にデータを記録する際の具体的な処理内容の一例を示す図である。

【図１１】

上記不揮発性メモリ情報記録媒体にデータを記録する際の具体的な処理内容の別の一例を示す図である。

【図１２】

上記不揮発性メモリ情報記録媒体からデータを再生する際の具体的な処理内容の一例を示す図である。

【図１３】

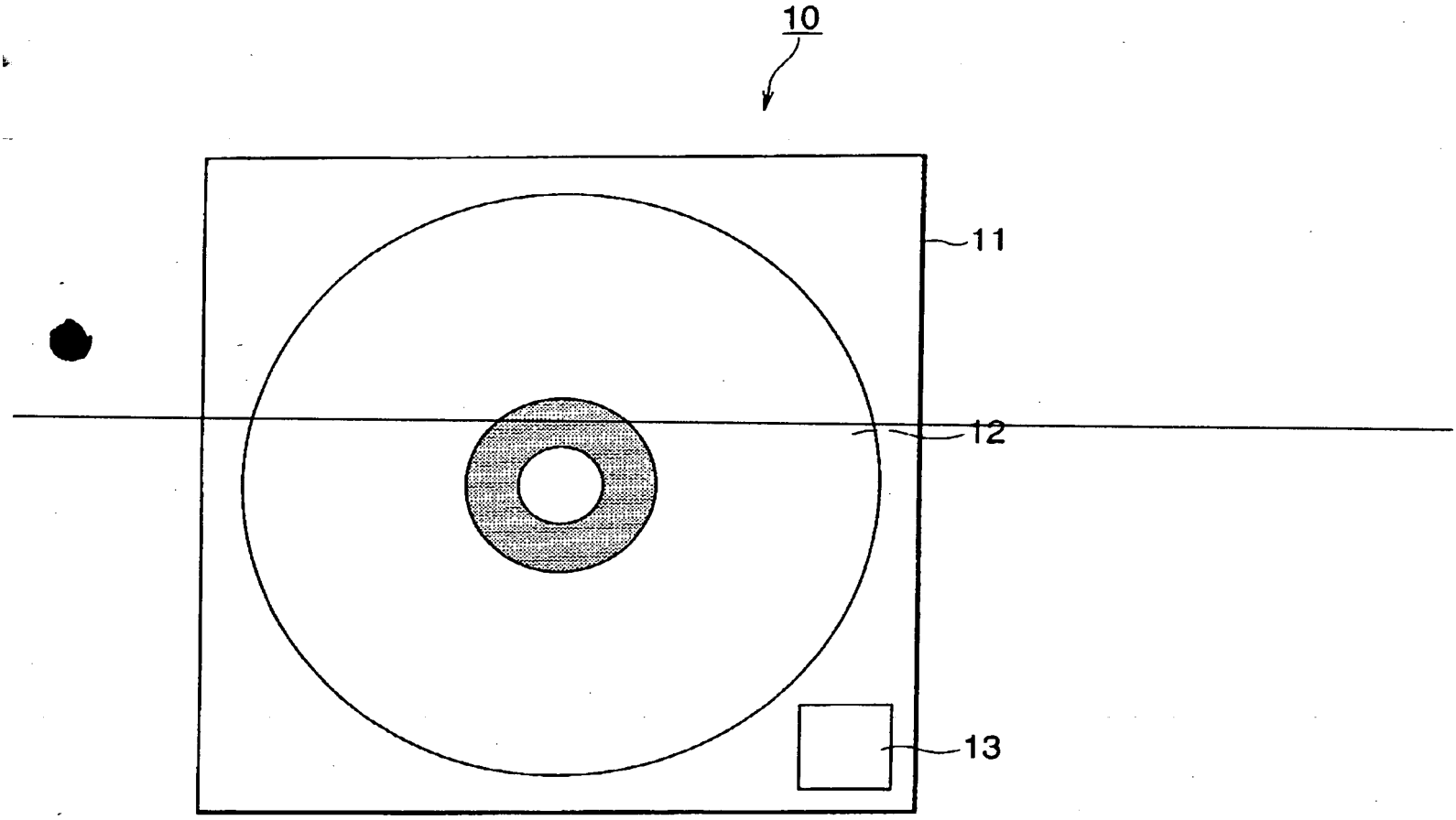
上記不揮発性メモリ情報記録媒体にデータを再生する際の具体的な処理内容の別の一例を示す図である。

【符号の説明】

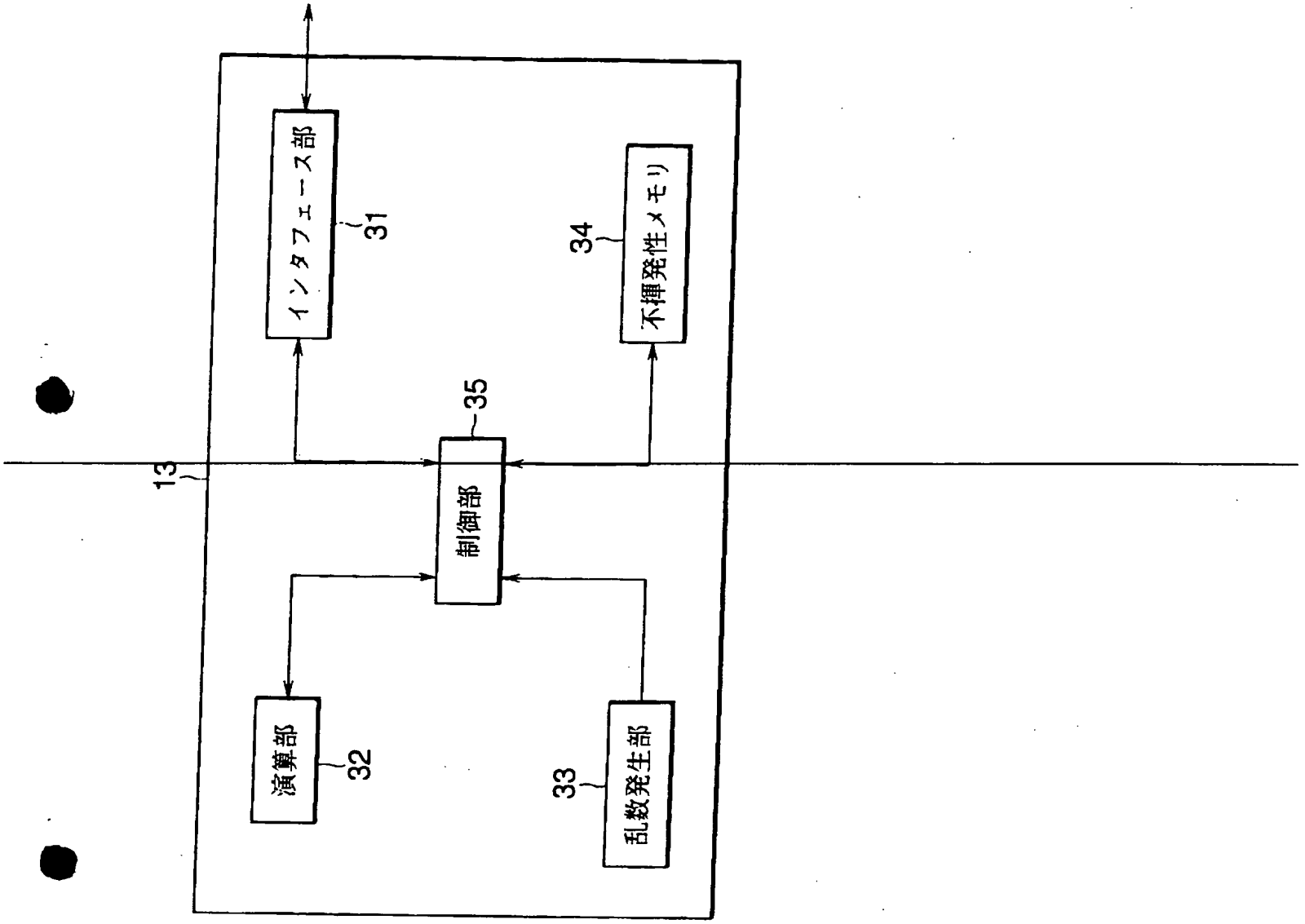
１０　光ディスク情報記録媒体、１１　カートリッジ、１２　光ディスク、１３　セキュリティモジュール、３１　インタフェース部、３２　演算部、３３　乱数発生部、３４　不揮発性メモリ、３５　制御部、１００　光ディスク記録／再生装置、１０１　スピンドルモータ、１０２　光学ヘッド、１０３　サーボ回路、１０４　記録／再生回路、１０５　制御部、１０６　入力部、１０７　乱数発生部、１０８　インタフェース部、１０９　演算部１０９、１１０　不揮発性メモリ、２０　不揮発性メモリ情報記録媒体、２１　カートリッジ、２２　不揮発性メモリ、２３　セキュリティモジュール、２４　入出力端子、４１　外部インタフェース部、４２　演算部、４３　乱数発生部、４４　不揮発性メモリ、４５　制御部、４６　記録媒体インターフェース部、２００　記録／再生装置、２０１　入出力端子、２０５　制御部、２０６　入力部、２０７　乱数発生部、２０８　インタフェース部、２０９　演算部、２１０　不揮発性メモリ

【書類名】　図面

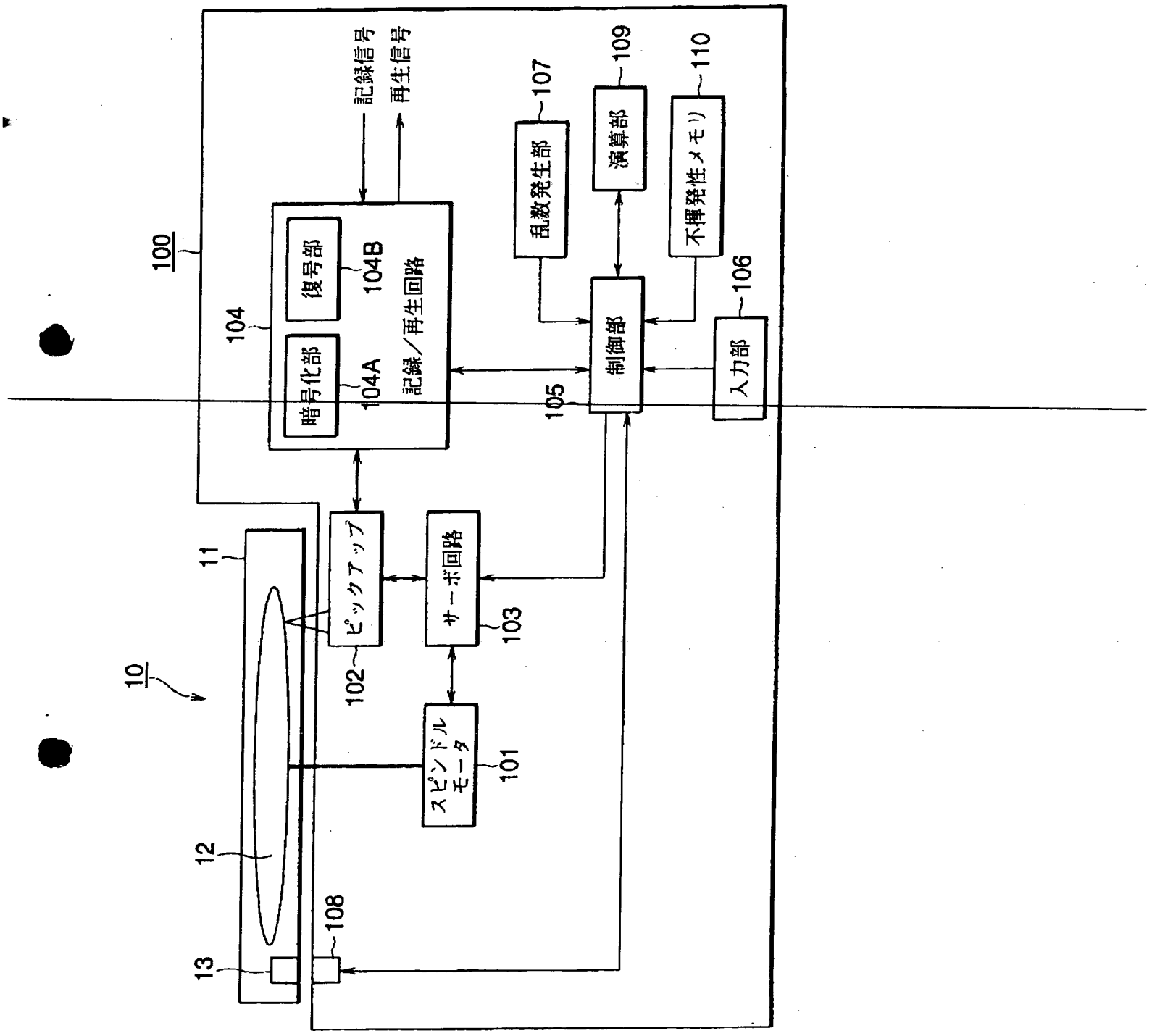
【図１】



【図２】



【図３】

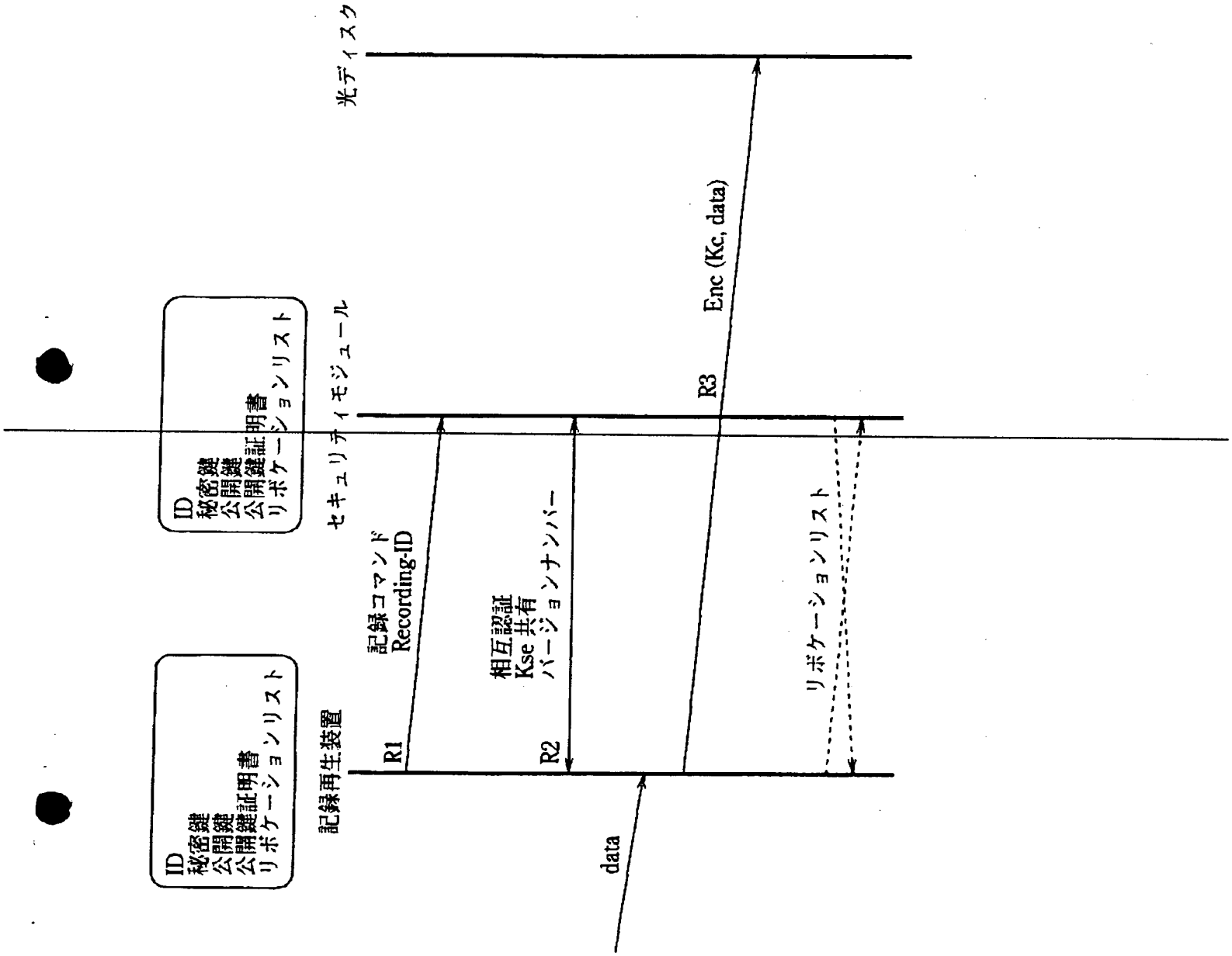

100
記録信号
再生信号
104
復号部
104B
暗号化部
104A
記録／再生回路
乱数発生部
107
演算部
109
不揮発性メモリ
110
制御部
105
入力部
106
ピックアップ
102
サーボ回路
103
スピンドルモータ
101
10
11
12
13
108

【図４】

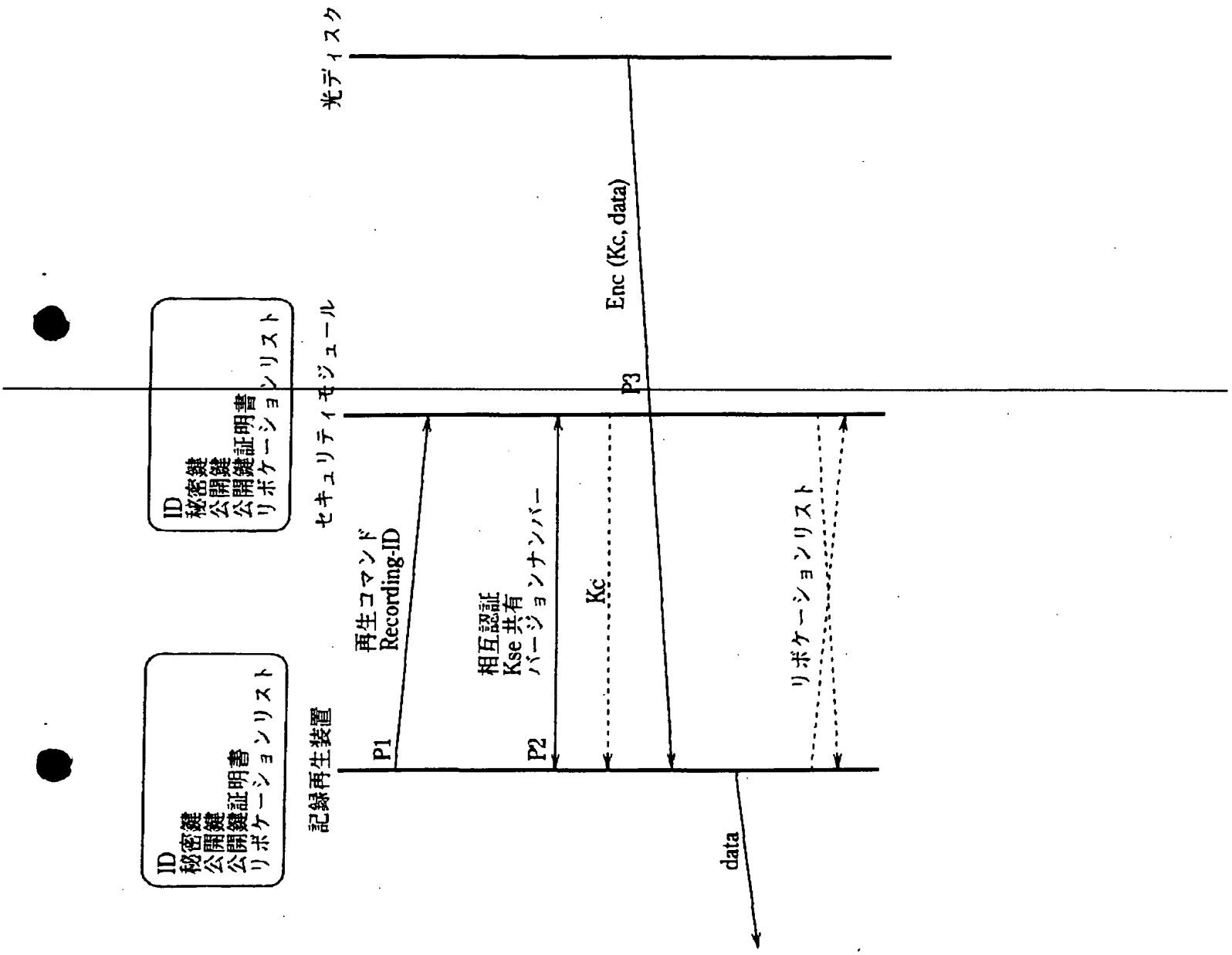
リボケーションリスト

バージョンナンバー
リボークされる機器または媒体のID
...
TCのデジタル署名

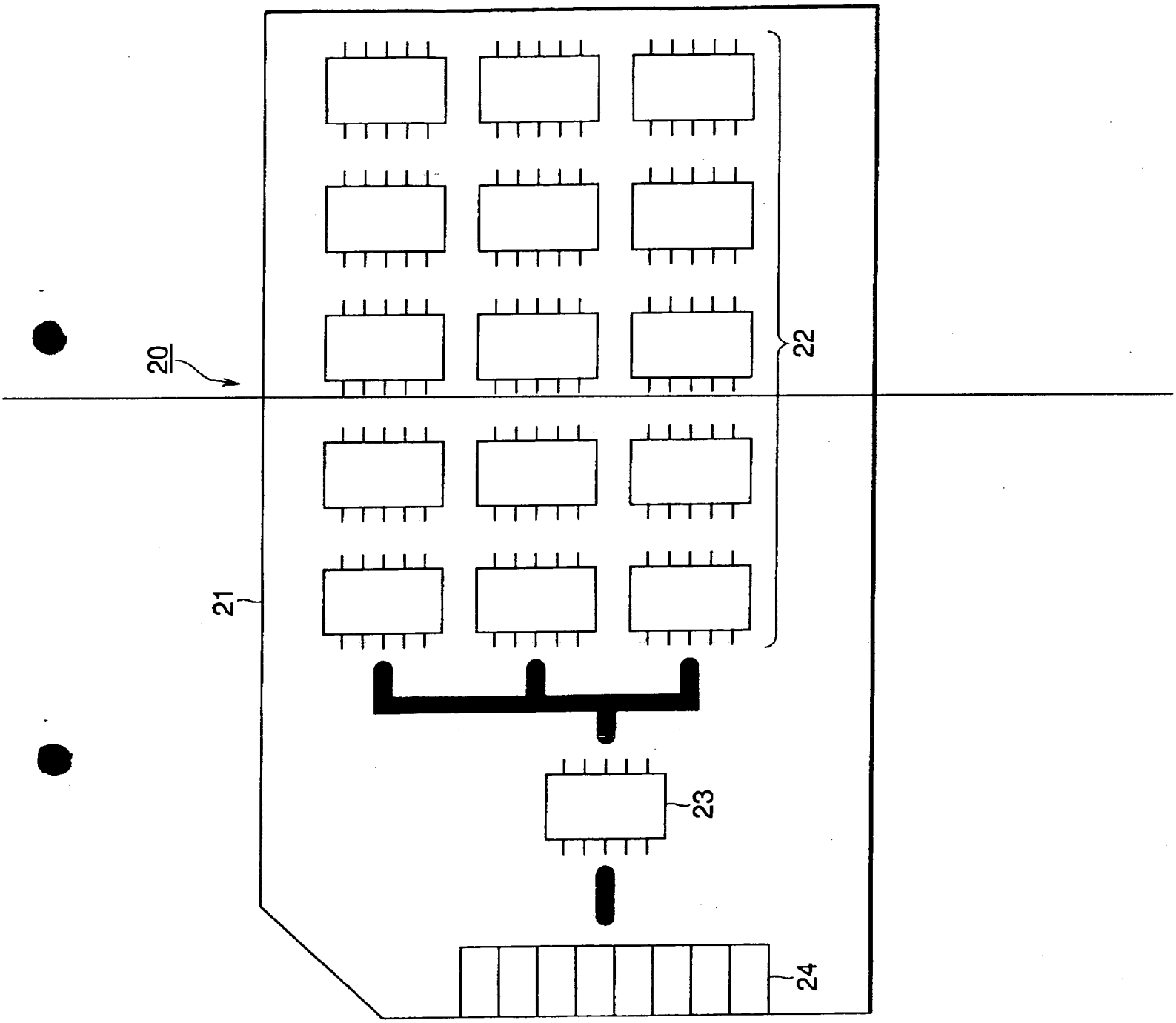
【図５】


光ディスク
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
セキュリティモジュール
Enc (Kc, data)
R3
記録コマンド
Recording-ID
R1
相互認証
Kse 共有
バージョンナンバー
R2
リボケーションリスト
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
記録再生装置
data

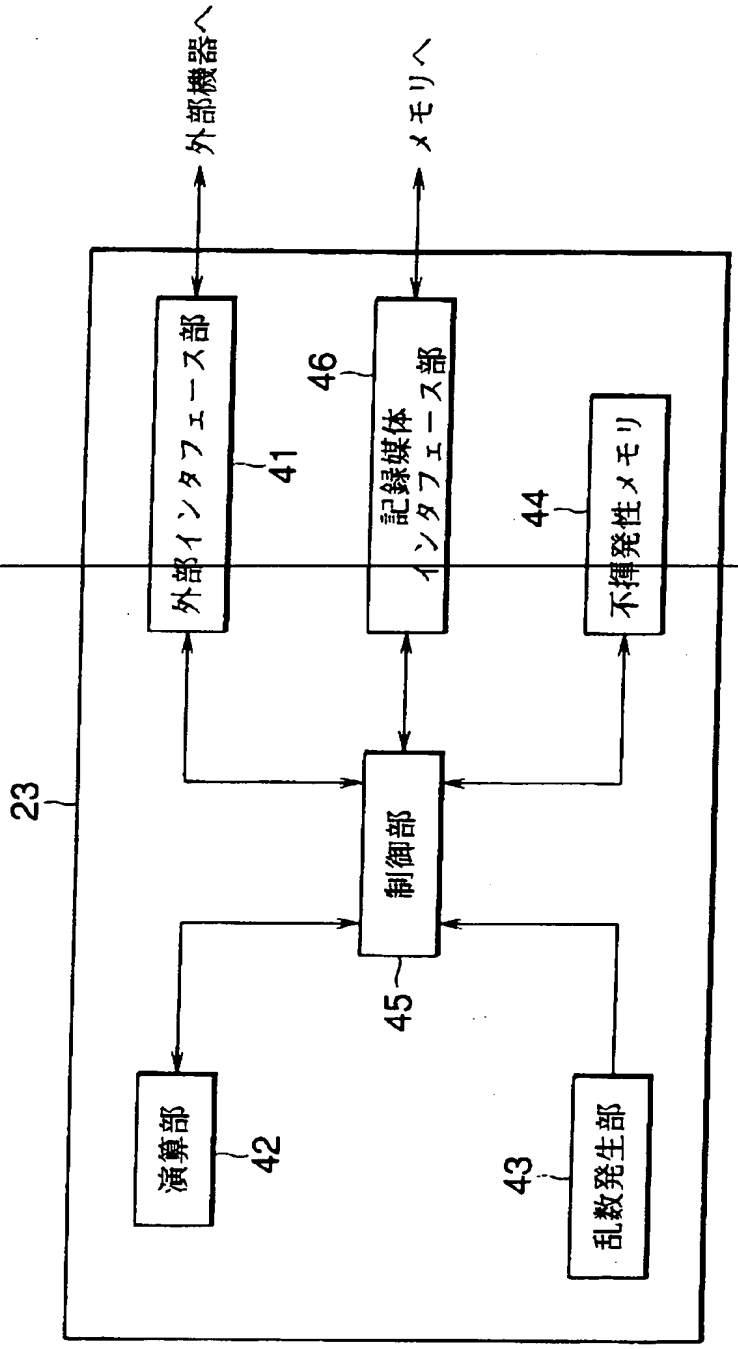
【図６】


光ディスク
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
セキュリティモジュール
Enc (Kc, data)
P3
再生コマンド
Recording-ID
相互認証
Kse 共有
バージョンナンバー
Kc
リボケーションリスト
P1
P2
記録再生装置
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
data

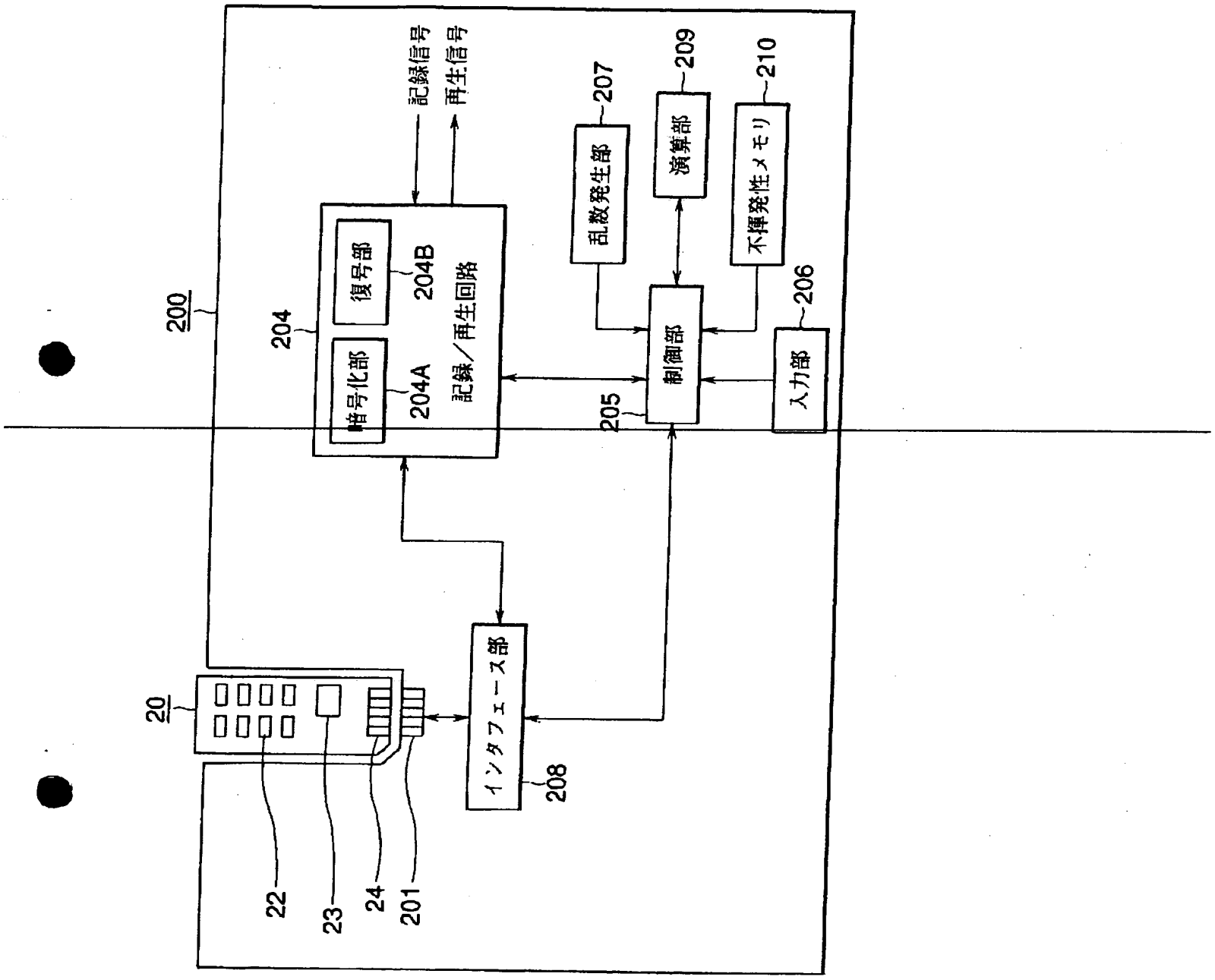
【図７】



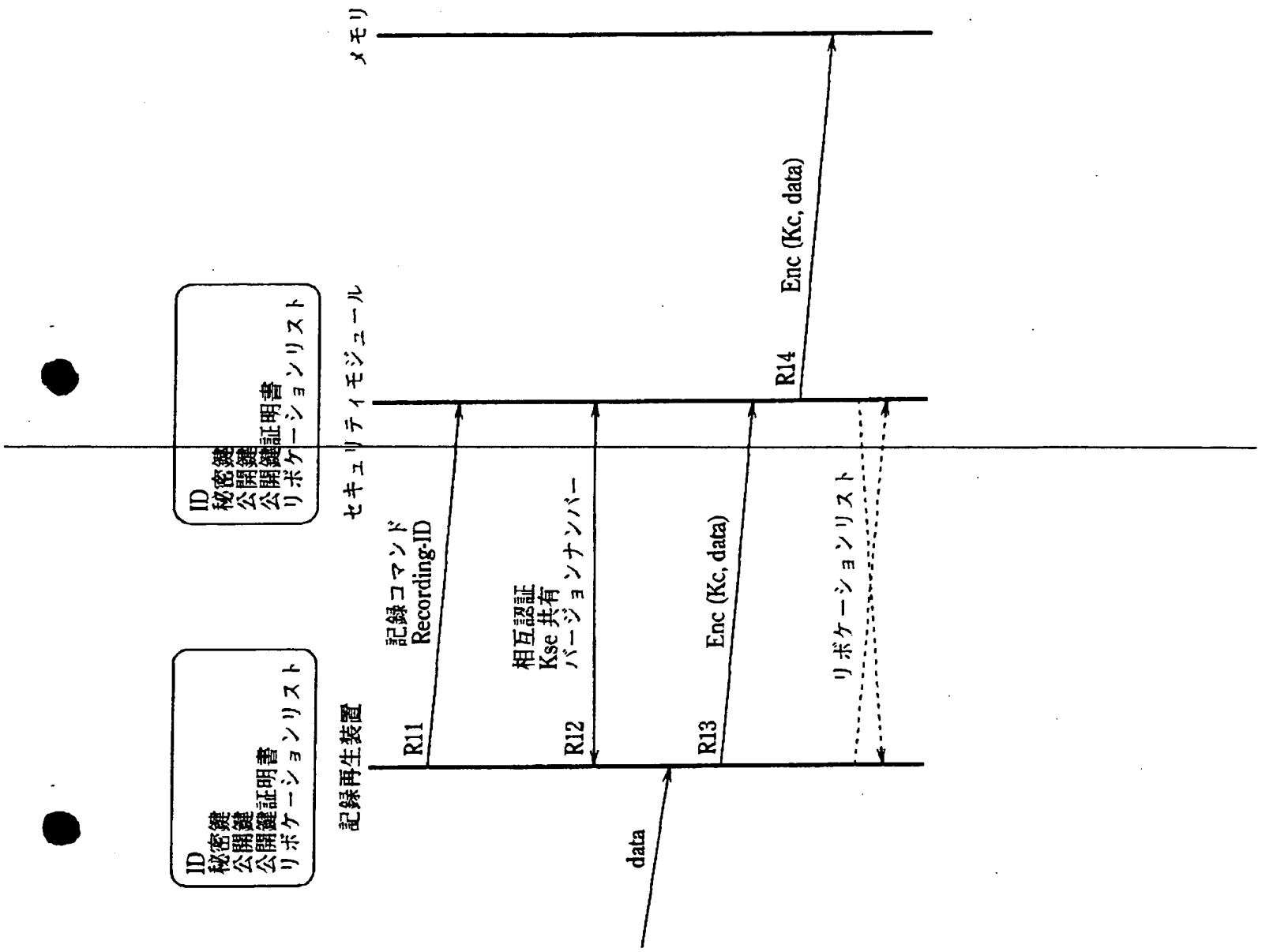
【図８】


外部機器へ
メモリへ
外部インタフェース部
41
記録媒体
インタフェース部
46
不揮発性メモリ
44
23
制御部
45
演算部
42
乱数発生部
43

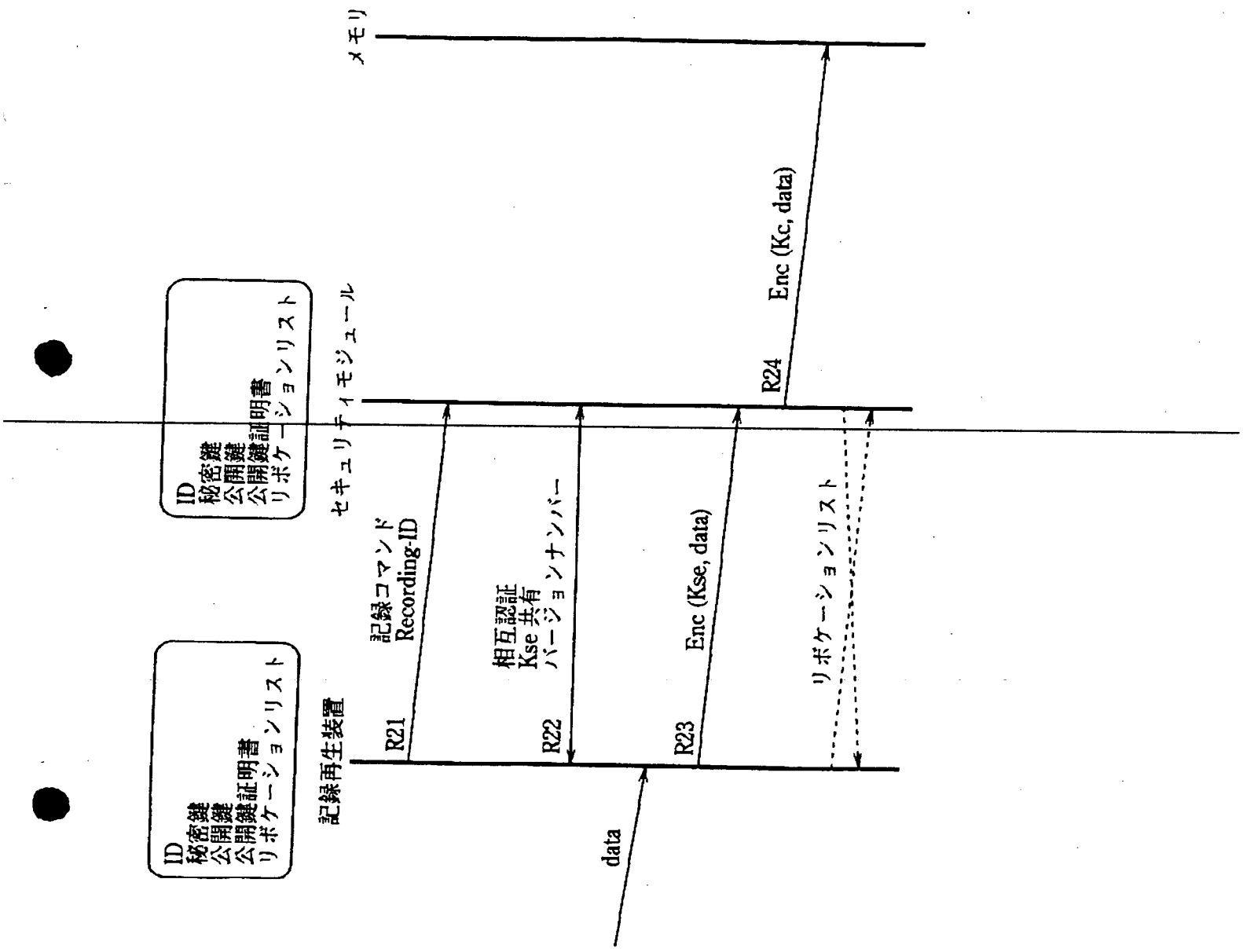
【図９】


200
204
暗号化部
204A
復号部
204B
記録／再生回路
記録信号
再生信号
乱数発生部
207
演算部
209
不揮発性メモリ
210
制御部
205
入力部
206
インタフェース部
208
20
22
23
24
201

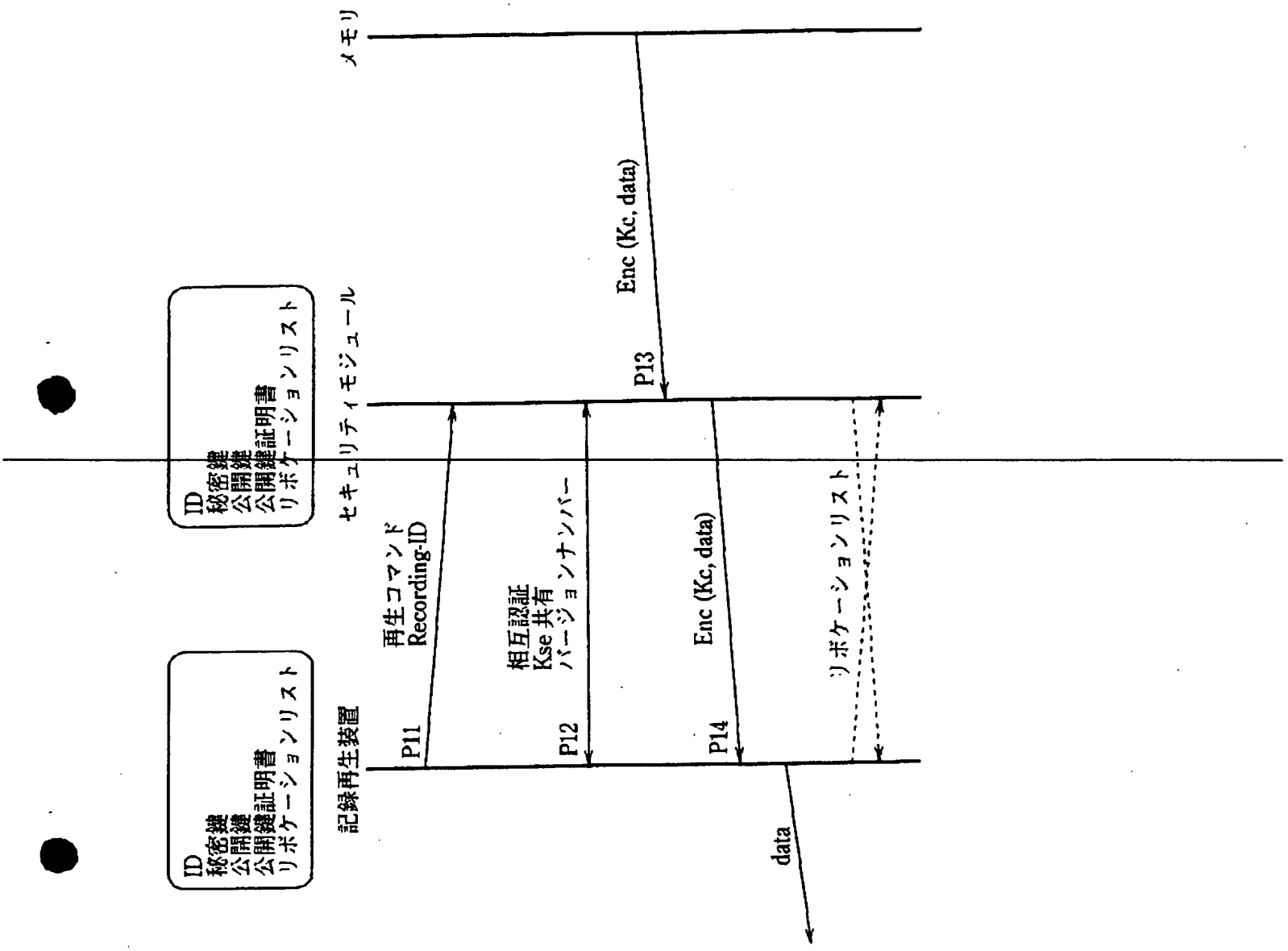
【図１０】


メモリ
セキュリティモジュール
記録再生装置
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
記録コマンド
Recording-ID
R11
相互認証
Kse 共有
バージョンナンバー
R12
Enc (Kc, data)
R13
Enc (Kc, data)
R14
リボケーションリスト
data

【図１１】


メモリ
セキュリティモジュール
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
記録再生装置
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
R21
記録コマンド
Recording-ID
R22
相互認証
Kse共有
バージョンナンバー
R23
Enc (Kse, data)
R24
Enc (Kc, data)
リボケーションリスト
data

【図１２】


メモリ
セキュリティモジュール
記録再生装置
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
再生コマンド
Recording-ID
P11
相互認証
Kse 共有
バージョンナンバー
P12
Enc (Kc, data)
P13
Enc (Kc, data)
P14
リボケーションリスト
data

【図１３】


メモリ
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
セキュリティモジュール
Enc (Kc, data)
P23
再生コマンド
Recording-ID
相互認証
Kse 共有
バージョンナンバー
Enc (Kse, data)
リボケーションリスト
ID
秘密鍵
公開鍵
公開鍵証明書
リボケーションリスト
記録再生装置
P21
P22
P24
data

【書類名】　　要約書

【要約】

【課題】　映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができるようする。

【解決手段】

光ディスク情報記録媒体１０にセキュリティモジュール１３を持たせ、光ディスク上に記録されるデータを個々のデータごとに異なる暗号鍵で暗号化し、暗号鍵をセキュリティモジュール１３が安全に保管する。また、セキュリティモジュール１３は記録／再生装置と公開鍵暗号技術を用いた相互記証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにする。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社